

IN THE UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MARYLAND
Northern Division

In the Matter of the Search of)	16 - 3205 - ADC
Electronic Account Stored at Premises)	Case No. _____
Controlled and Hosted by Facebook)	
headquartered in Menlo Park,)	<u>UNDER SEAL</u>
California)	

In the Matter of the Search of)	16 - 3206 - ADC
Electronic Account Stored at Premises)	Case No. _____
Controlled and Hosted by Twitter)	
headquartered in San Francisco,)	<u>UNDER SEAL</u>
California)	

In the Matter of the Search of)	16 - 3207 - ADC
Electronic Accounts Stored at Premises)	Case No. _____
Controlled and Hosted by Google)	
headquartered in Mountain View,)	<u>UNDER SEAL</u>
California)	

In the Matter of the Search of)	16 - 3208 - ADC
Electronic Accounts Stored at Premises)	Case No. _____
Controlled and Hosted by Skype,)	
which accepts service of process in)	<u>UNDER SEAL</u>
Redmond, Washington)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Special Agent Kyra Dressler, being duly sworn, hereby declare and state:

A. Introduction and Agent Background

1. I make this affidavit in support of an application for search warrants for certain social media and email accounts described further in Attachments A, B, C, and D (the “**Target Accounts**”) for the items described therein and per the guidelines described in Attachment E.

2. As set forth herein, there is probable cause to believe that on the computer systems

of the providers for the **Target Accounts**, there exists evidence concerning violations of 18 U.S.C. § 2339B (providing material support of a terrorist organization) and 18 U.S.C. § 2339C (unlawful financing of terrorism). This affidavit is made in support of applications for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the service providers to disclose to the government records and other information in their possession, pertaining to the subscribers or customers associated with the **Target Accounts**. Investigators have requested that the service providers preserve records for each of the **Target Accounts**.

3. I am a Special Agent with the Federal Bureau of Investigation ("FBI") currently assigned to the Baltimore Division of the FBI, Joint Terrorism Task Force ("JTTF") and have been so since 2009. As an FBI Agent, my responsibilities have included investigating a variety of criminal offenses, including drug trafficking, violent gang activities, and terrorism-related violations. In the course of my employment with the FBI, I have received extensive training in conducting criminal and counterterrorism investigations and I have authored affidavits in support of search and arrest warrants and testified in Federal trials.

B. Basis for Facts Contained in this Affidavit

4. I make this affidavit, in part, based on personal knowledge derived from my experience, training, and participation in this investigation and, in part, based upon information from the following sources: a) oral and written reports about this investigation and others that I have received from law enforcement officers, including Special Agents with the FBI, local law enforcement officials, and law enforcement authorities in the UK; b) communications, including telephone calls, faxes and emails obtained through criminal process; c) a review of internet login history and internet protocol addresses for services provider accounts; and d) information obtained during searches and witness interviews.

5. Except where otherwise noted, the information set forth in this affidavit is within my personal knowledge, or has been provided to me by law enforcement officers. I have not set forth each and every fact learned during the course of this investigation. Rather, I have set forth only the facts that I believe are necessary to establish probable cause for the issuance of the search and seizure warrants requested in this affidavit.

C. Facebook and Related Services

6. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. Subscribers to Facebook may access their accounts on servers maintained and/or owned by Facebook, from any computer connected to the internet located anywhere in the world.

7. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact email addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account. Facebook does not verify the information provided.

8. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual

Facebook users by sending each user a “Friend Request.” If the recipient of a “Friend Request” accepts the request, then the two users will become “Friends” for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user’s account includes a list of that user’s “Friends” and a “News Feed,” which highlights information about the user’s “Friends,” such as profile changes, upcoming events, and birthdays. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

9. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create “lists” of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

10. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. In addition, Facebook users can “check in” to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or

her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

11. Facebook allows users to upload photos and videos. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

12. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient’s “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

13. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages. Facebook also has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

14. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

15. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

16. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that user's access or use of that application may appear on the user's profile page.

17. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the

administrator and/or creator of the group. Facebook uses the term “Group Contact Info” to describe the contact information for the group’s creator and/or administrator, as well as a PDF of the current status of the group profile page.

18. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

19. Facebook retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

20. Facebook also retains information about their users, including that listed in Attachment A, Section II. Information and files stored on a Facebook server by a subscriber may not necessarily be located in the subscriber’s home computer. The subscriber may store electronic communications and/or other files on the Facebook server for which there is insufficient storage space in the subscriber’s computer and/or which he/she does not wish to maintain in the computer

in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the Facebook server.

21. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

22. Therefore, the computers of Facebook are likely to contain all the material described above. I know from training and experience that such information can provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, including evidence establishing and proving the elements of the criminal offense being investigation, or alternatively, excluding the innocent from further suspicion. I also know from my training, knowledge, and experience, that those involved in terrorist-related activities use Facebook to communicate with their criminal associates through Facebook chat functions, as well as through the posting of messages and videos for sharing with each other and other like-minded individuals, which support their terrorist-related beliefs and goals.

D. Twitter and Related Services

23. Twitter owns and operates a free-access social-networking website of the same

name that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to create and read 140-character messages called “Tweets,” and to restrict their “Tweets” to individuals whom they approve. These features are described in more detail below.

24. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

25. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user’s full name, email addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user’s profile was created, the date and time at which the account was created, and the IP address at the time of sign-up. Twitter keeps IP logs for each user. These logs contain information about the user’s logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile. This type of information can help to identify which computers or other devices were used to access a given Twitter account.

26. A Twitter user can post a personal photograph or image (also known as an “avatar”) to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post “bios” of 160 characters or fewer to their profile pages.

27. As discussed above, Twitter users can use their Twitter accounts to post “Tweets” of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also “favorite,” “retweet,” or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a “mention” of the identified user. In the “Connect” tab for each account, Twitter provides the user with a list of other users who have “favorited” or “retweeted” the user’s own Tweets, as well as a list of all Tweets that include the user’s username (i.e., a list of all “mentions” and “replies” for that username).

28. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services. Twitter users can also opt to include location data in their Tweets, which will reveal the users’ locations at the time they post each Tweet. This “Tweet With Location” function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data. Additionally, when Twitter users want to post a Tweet that includes a link to a website, they can use Twitter’s link service, which converts the longer website link into a shortened link that begins with <http://t.co>. This link service measures how many times a link has been clicked.

29. A Twitter user can “follow” other Twitter users, which means subscribing to those users’ Tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user’s “followers” list) and a list of people whom that user follows (i.e., the user’s “following” list). Twitter users can “unfollow” users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are

visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into “lists” that display on the right side of the user’s home page on Twitter. Twitter also provides users with a list of “Who to Follow,” which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

30. In addition to posting Tweets, a Twitter user can send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter’s database.

31. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user’s mobile phone, and the user can also set up a “sleep time” during which Twitter updates will not be sent to the user’s phone. Twitter also includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches. Twitter users can also connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users’ public Twitter profiles. If a Twitter user does not want to interact with another user on Twitter, the first user can “block” the second user from following his or her account.

32. Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the

user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

33. Thus, the computers of Twitter are likely to contain all the material described above. As is the case with Facebook, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation. A Twitter user's account information, IP log, stored electronic communications, and other data retained by Twitter can indicate who has used or controlled the Twitter account and how and when it was accessed or used. Additionally, by reviewing Twitter's IP logs for a particular account, investigators can determine the physical location associated with the logged IP addresses, and thereby learn the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to "tweeted" communications. This geographic and timeline information may tend to either inculcate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner's state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

E. Gmail and Related Services

34. Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email accounts identified in Attachment C, Section I. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information, which is significant to identifying those using and/or accessing the account.

35. A Google subscriber can store files with the provider in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

36. I know from my training and experience that email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Such information may constitute evidence of the crimes under investigation because it can be used to identify the account's user or users. Even if subscribers insert false information to conceal their identity, such information often provides clues to their identity, location or illicit activities.

37. I know from my training and experience that email providers typically retain certain transactional information about the creation and use of each account on their systems. This

information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP addresses used to register the account and associated with particular logins to the account. As previously stated, IP addresses can help to identify which computers or other devices were used to access the email account.

38. Email account users will often communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

39. As previously stated, information stored in connection with an electronic account, such as an email account, provides crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, including identifying individuals using or accessing the account, their geographic location (based on IP addresses), and their state of mind as it relates to the offenses under investigation (to include motive, intent, and/or consciousness of guilt. Thus, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction

information, and account application information.

F. Skype and Related Services

40. Skype provides a variety of on-line services, including video, audio, text, and group messaging, to the public. Skype allows subscribers to obtain accounts that give them access to these services. Subscribers obtain an account by registering with Skype. During the registration process, Skype asks subscribers to provide basic personal information, which can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. I know from my training and experience that even if subscribers insert false information to conceal their identity, that information can often provide clues to their identity, location or illicit activities.

41. A Skype subscriber can store with the provider files in addition to messages, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to messages), and other files, on servers maintained and/or owned by Skype. In my training and experience, evidence of who was using a Skype account may be found in address books, contact or buddy lists, and attachments to messages, including pictures and files.

42. In my training and experience, messaging providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account

(such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, messaging providers often have records of the IP addresses used to register the account and associated with particular logins to the account, which can help to identify which computers or other devices were used to access the account.

43. In many instances, messaging account users communicate directly with a service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Messaging providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

44. Therefore, the computers of Skype are likely to contain stored electronic communications (including retrieved and unretrieved messages for Skype subscribers) and information concerning subscribers and their use of Skype services, such as account access information, transaction information, and account application information. As is the case with the other electronic service providers referenced above, the information stored in a Skype account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation.

G. Probable Cause

45. On October 15, 2004, the United States Secretary of State designated al-Qa'ida in Iraq ("AQI"), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization

(“FTO”) under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist under Section 1(b) of Executive Order 13224. On May 15, 2014, the Secretary of State amended the designations for AQI to add the alias Islamic State of Iraq and the Levant (“ISIL”) as the organization’s primary name. The Secretary also added the following aliases to the ISIL listing: the Islamic State of Iraq and al-Sham (“ISIS”), the Islamic State of Iraq and Syria (“ISIS”), ad-Dawla al-Islamiyya fi al-‘Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the ISIL listing: Islamic State, ISIL, and ISIS. Although the group has never called itself “Al-Qaeda in Iraq (AQI),” this name has frequently been used to describe it through its history. In an audio recording publicly released on June 29, 2014, ISIS announced a formal change of its name to the Islamic State (“IS”). Beginning in 2014, using social media, ISIL has called for attacks against citizens—civilian and military—of the countries participating in the United States-led coalition against ISIL. For instance, on September 21, 2014, ISIL released a speech of Abu Muhammed Al-Adnani, a senior leader and official spokesman of ISIL. In this speech, entitled, “Indeed Your Lord is Ever Watchful,” Al-Adnani calls on Muslims who support ISIL from around the world to “defend the Islamic State” and to “rise and defend your state from your place where you may be.” To date, ISIL remains a designated FTO.

46. On June 28, 2015, according to Western Union transactional records, a sum of \$1,000 (exclusive of transaction fees) was wire-transferred to Maryland resident Mohamed ELSHINAWY from a named individual located in Egypt. ELSHINAWY received the funds on the same date, after which he was observed by FBI surveillance agents driving to his local bank branch where he conducted a transaction at the drive-up ATM. A review of the bank’s records

confirm that ELSHINAWY made an \$800 cash deposit into his account at that time and subsequently transferred \$200 from that deposit to a joint account held with his wife.

47. On July 17, 2015, ELSHINAWY consented to a non-custodial interview by Baltimore FBI agents. Upon being questioned about the nature of the \$1,000 Western Union transfer, ELSHINAWY made a series of false statements: first, that the money had come from his mother in Egypt; and second, that the money was provided to purchase an iPhone for a friend. After being advised that making a false statement to law enforcement was a criminal offense for which he could face imprisonment, ELSHINAWY finally revealed that the money had come from an individual he believed to be an ISIL operative.

48. ELSHINAWY advised the interviewing agents that his initial contacts with ISIL operatives had been arranged by his childhood friend Tamer EL-KHODARY. ELSHINAWY stated that EL-KHODARY had fled to Syria after having been released from Egyptian custody following his arrest on terrorism-related offenses. ELSHINAWY indicated that a few months prior to the date of his interview, he and EL-KHODARY had been communicating on social media. During those communications, EL-KHODARY sought to connect ELSHINAWY with a member of ISIL. ELSHINAWY claimed that he agreed to the contact because he believed that he would be able to get some money from ISIL. ELSHINAWY began communicating with the ISIL operative, whose name he did not know (hereafter "unidentified ISIL operative"), utilizing a method of communication that I know, through my training and experience, has been used by ISIL members.

49. ELSHINAWY told the interviewing agents that he ultimately received a total of \$4,000 in two payments from the unidentified ISIL operative. The first payment of \$3,000 was

sent to him from a company in the United Kingdom on May 14, 2015, via eBay/Paypal. ELSHINAWY showed the interviewing agents the eBay/PayPal receipt of transaction on his laptop computer, which identified the UK company sending the payment as a company called Ibacstel Electronics. ELSHINAWY also confirmed that he received the transactional details of the later, \$1,000 Western Union transfer from the individual in Egypt whom he understood to be an ISIL operative (hereafter "Egyptian ISIL operative"). ELSHINAWY indicated that he did not know the identity of this individual.

50. ELSHINAWY provided the interviewing agents a phone number for the unidentified ISIL operative that he had obtained during the course of their communications. ELSHINAWY stated that he was instructed to use the monies he received from the unidentified ISIL operative for "operational purposes," which ELSHINAWY understood to mean causing destruction or conducting a terrorist attack in the United States. ELSHINAWY stated that the unidentified ISIL operative did not provide specific guidance as to what weapons to buy or how to conduct an attack, but the Draw Mohammed Contest in Texas was given as an example.¹ ELSHINAWY stated he knew the money he was sent was to fund a terrorist attack, but he claimed that he never intended to conduct such an attack. Rather, he claimed he saw an opportunity to make money and take it from "thieves," and felt that the FBI should reward him for what he had done. ELSHINAWY stated that he was instructed that if he ever determined he was under surveillance by law enforcement, he was to stop whatever activities he was doing in connection with executing an attack.

¹ During the July 17 interview, it was unclear as to when this particular communication occurred between ELSHINAWY and the unidentified ISIL operative. On May 3, 2015, two individuals attempted to attack and kill attendees at an art contest in Garland, Texas, depicting drawings of the Prophet Mohammed. The individuals were immediately killed by law enforcement officers as they attempted to launch their attack.

51. ELSHINAWY did not tell the investigating agents about all the money he received from individuals associated with ISIL – a total of at least \$8,700. In addition to the \$1,000 sent by the Egyptian ISIL operative via Western Union, a review of PayPal records indicates that ELSHINAWY concealed from the FBI at least \$3,500 of the \$7,700 in funds he received from Ibacstel Electronics between March and June 2015. The total identified PayPal payments (exclusive of processing fees) were received by ELSHINAWY as follows: \$1,500 on March 23; \$1,000 on April 16; \$1,000 on May 1; \$3,000 on May 14; and \$1,200 on June 7. (The accounts associated with those payments are discussed further below.)

52. The investigation revealed that eight days after ELSHINAWY received the March 23 payment from Ibacstel Electronics, he used the monies to purchase a laptop computer and cell phone. Further analysis of bank records for the dates surrounding ELSHINAWY's receipt of monies from ISIL revealed that: 1) at least \$1,350 of the funds received were spent for communication devices such as phones, calling cards, the laptop computer referenced above, a hotspot for internet access, and a private VPN network all of which were utilized in connection with receipt of the funds and other communications between ELSHINAWY and his criminal associates; 2) at least \$3,000 of the funds received was converted into cash by ELSHINAWY through ATM withdrawals that are neither traceable nor accounted for; and 3) a portion of the remaining funds received appear to have been used for personal expenses, though not all of those monies can be accounted for with certainty.

53. On December 11, 2015, FBI agents arrested ELSHINAWY on terrorism-related charges. On January 13, 2016, he was indicted by a federal grand jury on charges of: providing and attempting to provide material support and resources to a designated FTO (ISIL), and

conspiracy to do the same, in violation of 18 U.S.C. § 2339B; unlawful financing of terrorism, in violation of 18 U.S.C. § 2339C(a); and making material false statements, in violation of 18 U.S.C. § 1001. His case is currently pending trial scheduled for June 5, 2017.

ELSHINAWY's Dealings with Abdul SAMAD

54. On October 9, 2015, during execution of a federal search warrant at ELSHINAWY's Edgewood, Maryland, residence, FBI agents recovered, among other items, a handwritten note located in a desk drawer that included the following information: "money Gram number: 29370828," "send amount: £1076.82," "receive amount: 1499.99 USD," "exchange rate: 1.392985," "Total amount: Euro 1.130.82," and "sender details: Name: ABDUL SAMAD" with a listed address that was subsequently identified as SAMAD's residential address in Newport, GBR. Records were subsequently obtained from MoneyGram, via subpoena, relating to transaction number 29370828. The transaction was directed to ELSHINAWY on March 18, 2015, from the UK, where it was subsequently routed to a Minnesota address. The transaction stalled at that point and was ultimately unsuccessful. The money was returned to SAMAD, and he collected it on March 23, 2015, from the Corporation Road Post Office, Newport, South Wales.

55. Investigators also obtained and executed search warrants during the course of the investigation for ELSHINAWY's Facebook account and various email accounts. The materials obtained pursuant to these warrants did not include any communications between ELSHINAWY and SAMAD. However, agents identified other means of communication that ELSHINAWY used to communicate with his criminal associates, some of which are unrecoverable, including electronic communications with his ISIL associates that ELSHINAWY took steps to conceal and ensure they were unrecoverable. Thus, ELSHINAWY may have used a covert method to discuss

the details of the MoneyGram transaction on the note recovered from his residence.

56. On December 10, 2015, SAMAD was arrested in the UK on a charge under British law of suspicion of arranging funds for the purposes of terrorism, and his UK residence and the UK office of Ibacstel Electronics and its associated companies (hereafter "IBACS") were searched. SAMAD's case is pending and he is presently on pre-charge conditional police bail.

57. As a part of the UK searches, SAMAD's laptops and electronic devices were seized and searched. On one of SAMAD's seized laptops (the gold laptop), an official, scanned, color-copy of the March 23, 2015, attempted MoneyGram money transfer to ELSHINAWY was discovered. Additional details were provided by SAMAD on the official MoneyGram document, which included his date, phone number and residential address. Following ELSHINAWY's arrest on December 11, 2015, his residence was searched for a second time. During that search, the official MoneyGram receipt was located for the attempted money transfer between ELSHINAWY and SAMAD. This receipt matched the date, name, address, and amount of the handwritten note found in October 2015 in ELSHINAWY's desk drawer.

58. SAMAD was interviewed by UK law enforcement officials following his arrest. During those interviews, he spoke about his employment with IBACS and his relationship with Siful SUJAN, who started the company, and SUJAN's brother, Ataul HAQUE, who was a Director of the company. SAMAD said SUJAN hired him in November 2013 as an assistant who answered calls and took care of customer orders, among other things. He indicated that IBACS developed websites, and obtained and configured printers (obtained from China), for their customers' businesses. Eventually, SUJAN and HAQUE made him Director of the Cardiff office. In that role, SAMAD was responsible for making payments to individuals at the direction of SUJAN and

HAQUE, whom SAMAD stated were both traveling setting up an office in Turkey and running the IBACS office in Dhaka, Bangladesh. SAMAD said he had full access to all IBACS financial accounts and emails, in addition to full reign over company operations.

59. When he was arrested, SAMAD asked the arresting officers if his arrest was in relation to a business account. During his initial interview, SAMAD explained that he had asked that question because at some point in 2014 he became suspicious of certain transactions he was directed to conduct that involved people not related to IBACS business. He stated that SUJAN developed the “type of Islam” that was “aggressive and angry” a few months prior to leaving the UK to return to Bangladesh and expressed his belief to SAMAD that killing innocent people was justified. Despite his concerns about SUJAN’s mindset, SAMAD elected to stay with the company because HAQUE promised to make him a company Director. SAMAD stated that SUJAN never talked about conducting violent acts, but did suggest that violence was justified as a means to oppose the western governments. SAMAD indicated his belief that SUJAN would elect to conduct harm by way of operating behind computers because that was his training and expertise. Other than showing SAMAD pictures of extreme Muslims, SUJAN did not try to radicalize him. SAMAD stated that in light of SUJAN’s “aggressive Islam hate preaching,” he believed it likely that SUJAN was probably located somewhere with ISIS and no longer in Turkey.

60. On December 10, 2015, SUJAN was killed in Raqqa, Syria. He was publicly confirmed by the United States military to be a computer hacker for ISIL and its director of computer operations. UK investigators uncovered a December 2015 chat communication on one of SAMAD’s seized cell phones that occurred between SAMAD and HAQUE (using an alias that SAMAD identified during his police interviews as belonging to HAQUE) on a secure

communication platform. HAQUE told SAMAD that “they” know where “sif” was located and that members of their [HAQUE and SUJAN’s] family had been arrested or questioned. I believe, based on my knowledge of the investigation, that HAQUE was referencing a law enforcement operation conducted in early December 2015 by law enforcement authorities in Bangladesh against the Bangladesh office of IBACS. Shortly thereafter, as previously stated, SUJAN was killed in Raqqa, Syria, on December 10, 2015.

61. The electronic media seized by the UK from SAMAD and the IBACS office were found to contain troves of financial and business records for IBACS. UK authorities discovered matching records of PayPal payments to ELSHINAWY, beginning with a payment of \$1,500 sent to ELSHINAWY via PayPal on March 23, 2015, to replace the failed MoneyGram transfer attempted by SAMAD. The first four PayPal payments from IBACS to ELSHINAWY were directed to email address thecheapmart@gmail.com (associated with a business ELSHINAWY had registered). The fifth and final PayPal payment was directed to email address vwfanaticthatsme@gmail.com, which the investigation revealed is subscribed to Rachel Rowe, who is ELSHINAWY’s co-habitant and whom he refers to as his Islamic wife. A record of this last payment was found on SAMAD’s laptop within a folder for the ibacsgroup.com Google account associated with Ibacstel Electronics Ltd. The record reflected a PayPal payment of \$1,341.98 sent to vwfanaticthatsme@gmail.com for two Canon all in one laser printers. The seller was listed as vwfanaticthatsme@gmail.com, and the listed delivery address was the UK office address for IBACS at that time.

62. The two Canon printers allegedly associated with the last identified PayPal payment to ELSHINAWY appear to have been an attempt to conceal the fact that monies were being

transferred to ELSHINAWY by ISIL members. These two printers were never discovered in any of the searches of ELSHINAWY's or SAMAD's residence or business, and business records from PayPal associated with ELSHINAWY's accounts never revealed a confirmed shipment to him or his registered addresses, nor did any of ELSHIANWY's drop shipping accounts ever reveal a purchase of printers. During his non-custodial interviews with the FBI, ELSHINAWY admitted that he utilized a method called "drop-shipping" to make it appear as though products were being purchased and shipped to his ISIL associates in exchange for the monies being sent by them to the United States.

63. In the course of their investigation, UK authorities also discovered the use of a purchased virtual private network ("VPN") service by SAMAD, HAQUE, and SUJAN for IBACS, a service also found to be used by ELSHINAWY (as referenced above). Your affiant knows a VPN is used to ensure total anonymity and privacy while online. Instead of using a common search engine's network, such as Google or Yahoo, it is commonplace for those trying to conceal their online activities to utilize a VPN and/or proxy server. The investigation revealed that IBACS used a particular name-brand VPN to transfer the monies highlighted in this affidavit to ELSHINAWY.² Also located on SAMAD's laptops and on hard drives found in the IBACS office was a large quantity of ISIL and AQ propaganda commonly read, reviewed and maintained by terrorists, to include but not limited to Milestones and Milestones Special Addition, a propaganda martyrdom video with the ISIL flag, and several hundred speeches and/or videos from Anwar Aulaqi (a well-known, and now deceased, radical Sheikh who encouraged his acolytes to commit

² The website of this particular VPN provider tells potential customers who are seeking VPN services that "[u]sing a VPN is like having a PO box on the internet – an address that no one can trace back to you," and, thus, people "can't trace your activity back to your real address and find out who or where you are."

acts of terror against the West), in addition to evidence of various social media accounts accessed by SAMAD bearing extensive references to ideology and jihadist propaganda involving ISIL and Usama Bin Laden consistent with an Islamic extremist mindset.

64. In one folder titled, "Credentials," found on one of SAMAD's laptops, there was an Excel spreadsheet listing the details of financial accounts, servers and domains, social media accounts, company details, invoices, email accounts, and associated passwords, usernames and security passwords. During the course of interviews, SAMAD provided signed consent for the UK authorities to search a number of email and social media accounts to which he had access. As detailed below, information from those accounts has been reviewed and some information was captured. However, since the UK authorities were limited in the scope of what they were able to access and search, this affidavit seeks warrants to capture the full scope of information from those accounts that constitutes evidence and instrumentalities of the terrorism-related violations encompassed in the conspiracy for which ELSHINAWY has been indicted.

Google Accounts: info@ibacstel.com, info@ibacs.co.uk, ataul@ibacs.co.uk, ataul@ibacstel.com, and ataul03@gmail.com

65. A review of the seized electronic evidence revealed multiple email accounts used by IBACS that SAMAD configured in such a way to allow him to link the accounts together so they could be more easily managed. Two of these linked accounts were info@ibacstel.com and info@ibacs.co.uk.³

66. In January 2015, IBACS purchased two Centre Loaded Mag Mount Scanner Antennas from an electronic components company in the UK. This device is a long antenna

³ Google allows businesses or individuals to create email accounts using their own domain name --- e.g., "joe@yourcompany.com," as opposed to "joe@gmail.com." Here, the email accounts ending in "@ibacstel.com" and "@ibacs.co.uk" are Gmail accounts that use a personalized domain name.

equipped with a magnetic base that is often times affixed to a vehicle for reception and scanning of radio frequencies for a CB or HAM radio. HAQUE and SAMAD communicated with regard to the purchase and shipment of this item over the above-referenced email accounts. On January 14, 2015, HAQUE emailed SAMAD advising him that a small parcel would be arriving the next day, and he wanted SAMAD to ship it to Ahmet Bayaltun in Sanliurfa, Turkey, which is located approximately 20 miles from the Syrian border. HAQUE followed up with another email on January 25, 2016, directing SAMAD to ship the package to Turkey the next morning, which SAMAD did, via TNT. A copy of the shipping invoice – found on SAMAD’s laptop – identified SUJAN as the contact person for the sender, Ibacstel Electronics. The need for this particular type of antenna is inconsistent with the nature of IBACS’ business. According to their website, IBACS is a website design company specializing in website development, software development, electronic point of sale solutions, electronic point of sale retail systems and various other software and web application products. As SAMAD related in his police interviews, the company’s primary business involved purchasing handheld printers for businesses using its printer service.

67. In early February 2015, a PayPal account linked to HAQUE and his wife Ana Gonzalez (also an IBACS business partner) was used to purchase three “bug sweep units” from a company in Florida specializing in surveillance and tracking equipment. The particular units are advertised on the company’s website as a “GPS bug sweep, portable wire tap, 3G/4G cell phone and camera finder,” costing \$395 each, that will detect anything that emits a radio signal within a 35-40 foot radius. In an interview with FBI agents, the company’s president confirmed that the items were shipped to Ahmet Bayaltun in Sanliurfa, Turkey. As is the case with the antenna referenced above, the need for this type of surveillance unit is inconsistent with the nature of

IBACS's business.

68. In his interview, the Florida company's president indicated that he remembered this particular transaction because the circumstances were unusual and the products purchased were his own company brand, which is only available through the company's online store. The company president recalled that the ebay ID (Ataul83) used for the purchase, the name of the purchaser (Ana Gonzalez at anabadadjoz82@hotmail.com), and the recipient in Turkey were all different individuals. Additionally, a few days after the purchase, HAQUE contacted the Florida company using email address ataul03@gmail.com and asked to be supplied with a lower cost invoice. The information received from the Florida company and a review of records retrieved by UK authorities indicated that four different email addresses were used by the company to communicate with HAQUE to complete the transaction: ataul03@gmail.com, ataul@ibacstel.com, ataul@ibacs.co.uk, and info@ibacs.co.uk.

69. Between March 2015 and May 2015, HAQUE, conducting business as "Ibacstel Electronics Ltd" and using email accounts info@ibacstel.com and atual@ibacs.co.uk, exchanged emails with the Florida company regarding the purchase of additional bug sweep units to be shipped to the same individual and address in Turkey referenced above and paid for through the Ibacstel Electronics PayPal account. During the exchange of emails with the company, HAQUE was advised that when using PayPal, the company could only ship to the confirmed address for payment, which in this case was the UK address for IBACS. The President of the Florida company advised the FBI that payment for the products was refunded to IBACS pending the address correction in PayPal, or payment through wire transfers. In the end, the products were never shipped because HAQUE never complied in changing the address in PayPal or wiring the monies

to pay for the purchase.

70. Based on a review of the UK seized evidence and PayPal records, the account info@ibacstel.com was used to facilitate all of the payments from IBACS to ELSHINAWY between March and June 2015 (referenced above).

71. The info@ibacstel.com account also contained an email from PayPal services, dated March 13, 2015, that appears to be a confirmation email for a membership for the particular VPN service being utilized by IBACS. Between March 2015 and September 2015 there were numerous emails confirming monthly \$49.00 payments to this VPN provider, indicating a subscription to their service was purchased using this email account.

72. Located in SAMAD's seized electronic media were numerous Google Hangout chat sessions. Google Hangouts is a service provided by Google to its clients. Subscribers using Google Hangouts can text, call, video call, and send pictures and money through the application either using a computer, phone, or other mobile device.

73. UK investigators captured a screen shot of an email dated July 29, 2014, sent from SAMAD to username iBacs IT Solutions and email address ataul@ibacs.co.uk. In the email, SAMAD addressed "siful" specifically, asking him how much he wanted to sell his computer for and if there were any important files that he wanted backed up. Later that day, "me" at username iBacs IT Solutions replied back to SAMAD and "ataul" stating that he did need everything backed up and that they could talk while doing so. During his police interviews, SAMAD identified SUJAN's username as "iBacs IT Solutions." The nature of July 29, 2014, conversation and identification of the participants clearly confirms that SUJAN was using the username and email account associated with iBacs IT Solutions. Additionally, after reviewing the full content in the

Google Hangouts chat sessions captured by the UK authorities, there were several examples of both SUJAN and HAQUE exchanging password and username information with SAMAD to various other IBACS accounts. Thus, it is believed that SAMAD, HAQUE, and SUJAN had access to the group business accounts associated with IBACS.

74. On June 8, 2015, after receiving a PayPal confirmation receipt reflecting the alleged sale of two Cannon printers to IBACS via the ebay/PayPal account associated with ELSHINAWY's partner Rachel Rowe (see paragraph 61 above), SAMAD (using info@ibacstel.com), sent an email to HAQUE (at ataul@ibacs.co.uk) and HAQUE's brother-in-law (an employee in the IBACS' Bangladesh office) inquiring as to who had purchased the two Cannon printers. HAQUE responded stating, "Bro, I bought it. It will not [be] delivered to UK office. I will let you know later insallah." As previously noted, the Cannon printers were never purchased, and instead, were likely utilized as a cover to transfer funds to ELSHINAWY to be used to commit a terrorist attack on behalf of ISIL.

75. In a Google Hangouts chat session on June 12, 2015, HAQUE (under the name "ataul haque") told SAMAD (using info@ibacstel.com), "you will get it at info@ibacs.co.uk," indicating SAMAD had access to the info@ibacs.co.uk account. HAQUE then stated, "check the google drive." A few minutes later, SUJAN replied, "which folder?" indicating he was a participant in the chat session between SAMAD and HAQUE. Your Affiant knows that one of Google's services is "Google drive." Each Google account has a corresponding "drive" account, which is similar to that of a digital cloud. Thus, it appears that SAMAD, HAQUE and SUJAN were not only participants in the chat session, but also all had access to both the info@ibacstel.com and info@ibacs.co.uk email accounts.

76. The IBACS business accounts (info@ibacstel.com and info@ibacs.co.uk) are further linked to SAMAD, HAQUE, and SUJAN through their use of corresponding usernames and icons/avatars associated with the accounts. A screen shot capture of SAMAD's Google Hangouts login screen revealed the username "iBacs Technologies Ltd" and "iBacs" with respect to certain chat communications. Located in a folder in the email account samad@ibacs.co.uk were the identical communications between SAMAD and username "iBacs IT Solutions Ltd." It appears that the Google Hangout chat sessions were conducted on SAMAD's mobile device or computer and then stored in the corresponding email account in the appropriate folder. Located in the Google Hangouts account associated with samad@ibacs.co.uk (discussed below) was a folder titled "iBacs Group," which is where the chat sessions discussed further in this affidavit were observed.

77. Based on the above information, I believe probable cause exists to believe that the Gmail accounts info@ibacstel.com, info@ibacs.co.uk, ataul@ibacstel.com, ataul@ibacs.co.uk, and ataul03@gmail.com, contain information about the money transfers to ELSHINAWY and other IBACS business transactions relevant to the charged terrorism conspiracy, to include the support of ISIL.

Google account: samad@ibacs.co.uk

78. Located on SAMAD's seized cell phone was a screen shot capture of an active login to SAMAD's Google account samad@ibacs.co.uk. As discussed above, several Google Hangouts chat sessions between SAMAD, using this account, and usernames iBacs IT Solutions and iBacs Technologies were discovered during the review of the account's content. The usernames iBacs IT Solutions and iBacs Technologies are associated with the iBacs group account

to which both SUJAN and HAQUE had access. The icon or avatar for usernames iBacs IT Solutions and iBacs Technologies is an orange and grey geometric pattern. This same icon/avatar was also observed to be associated with SUJAN's Google accounts (discussed below). In a number of instances, a chat session captured on SAMAD's phone would reference the opposing speaker utilizing username iBacs Technologies, while the exact same chat session captured in the email account would reference the opposing speaker's username as iBacs IT Solutions. As previously noted, SAMAD identified SUJAN's username as iBacs IT Solutions.

79. On November 7, 2014, SUJAN (using his username iBacs IT Solutions) copied an email to SAMAD from a potential IBACS customer. The forwarded email was addressed as follows: "Hello Mr. Sujan..." SUJAN asked SAMAD to contact the potential customer and then provided SAMAD his new phone number. SAMAD asked SUJAN if he was still using his old phone, to which SUJAN replied that he was only checking the voicemails and not to share the number with anyone. At this juncture, SUJAN had left the UK and, based on review of other electronic communications on the media seized in the UK, appeared to be in or near Turkey.

80. Also located in this email account was pro-ISIL, anti-West Islamic extremist propaganda. For example, on July 3, 2014, SAMAD (using samad@ibacs.co.uk) engaged in a Google Hangout conversation with SUJAN (using his username iBacs IT Solutions). SUJAN shared a web link to a PDF document titled "A Message to the Mujahidin and the Muslim Ummah in the Month of Ramadan," by Abu Bakr Al-Husayni Al Qurashi Al-Baghdadi (referred to herein as Al-Baghdadi, who is the self-proclaimed "Amir," or leader, of ISIL). The document encourages Muslims to join the Islamic State.

81. During a continuation of the chat later in the day, SUJAN stated, "first ever release

from him...” “original audio.” SUJAN then provided a link to the audio. SAMAD replied stating, “abu bakr?” and “akhi, where are you getting these from!? I need.” SUJAN replied “its” all over the internet, further suggesting SAMAD use Twitter to access the audio. SAMAD said he would create an account on the platform in order to do so. SAMAD stated he could not fully understand the video, since he had not finished his Arabic course. SUJAN also sent a web link to a BBC news article entitled “Iraq militant groups ordered to swear Isis allegiance.” The news article quoted Al-Baghdadi as stating, “...self-styled caliph of the Islamic State, Abu Bakr al-Baghdadi, has issued a call for jihadists around the world to flock to Syria and Iraq to fight and help build the state.” SAMAD sent a number of messages asking for information on who he should follow on the designated social media platform, to which he did not receive a response. However, soon thereafter, he advised SUJAN that he had figured it out and would follow the “ISIS Media Hub.” SUJAN responded with what appeared to be a password and username to access the account.

82. On July 7, 2014, SAMAD, using email account samad@ibacs.co.uk, engaged in another Google Hangout conversation with SUJAN, during which SUJAN sent a web link to a video titled “Ameerul Mumineen (Eng Translation).” I know from my experience and training that the term “Ameerul Mumineen” is Arabic for “leader or commander of the faithful.” Throughout Islam, some caliphs and other independent sovereign Muslim rulers have used this term as a title to claim legitimacy or leadership over a community of Muslims. Al-Baghdadi claimed this term in or around 2014 when he was hailed as the Amir or leader of the Islamic State or ISIL. The conversation continued with SUJAN advising SAMAD not to post in Facebook for security reasons. SAMAD laughed and said he hated not being able to do so. SUJAN admonished SAMAD that the latter could not forget he was in the UK and that ISIS is AQ and the government

scrutinizes those who show support for them. SAMAD ended the conversation by calling the government idiots.

83. On July 15, 2014, SUJAN sent SAMAD a video titled, “Amazing dream of Musa Jibril (Hafidhallah).” On July 25, 2014, he sent SAMAD a video titled, “Tawheed #1 – Explanation of three fundamental Principals – Shaykh Ahmad Jibril.” I know from my training and experience that Ahmad Musa Jibril is an ISIL supporter and Salafi Shaykh from Michigan. Jibril conducts online lectures that advocate jihad and adhere to the extremist ideology. This string of communications was stored in the samad@ibacs.com account in a folder titled “group hangout.” A screen capture of this chat session bore the name “siful sujan,” further confirming SUJAN as a participant in the chat.

84. Also found in the samad@ibacs.co.uk Google account was another folder titled “Directors/Ataul.” Inside that folder was a saved Google Hangouts chat session between SAMAD and HAQUE from March 17 through March 19, 2015, discussing the attempted MoneyGram transfer of funds to ELSHINAWY. More specifically, on May 17, 2015, HAQUE asked SAMAD if he had an account for a certain encrypted communication platform, to which SAMAD confirmed that he did and confirmed it was the same number. HAQUE told SAMAD to check it for an incoming message pertaining to the MoneyGram transfer, to which SAMAD confirmed the receipt of the message. HAQUE then confirmed that now SAMAD had the name and address for the transfer, which was clearly a reference to the recipient of the funds to be sent through MoneyGram – in this case, ELSHINAWY.

85. As the chat continued, SAMAD asked HAQUE if he could use an IBACS bank card, to which HAQUE suggested he should withdraw cash instead. SAMAD explained that he

did not want the bank to ask questions, and they discussed ways in which they could withdraw the money without alarming anyone. HAQUE told SAMAD to withdraw the cash from SAMAD's personal account that he would then be reimbursed for with monies from an IBACS bank account. Finally, HAQUE told SAMAD that he could use Western Union or MoneyGram in order to send the payment.

86. On March 18, 2015, SAMAD and HAQUE continued their chat regarding the attempted MoneyGram transfer to ELSHINAWY. HAQUE directed SAMAD to provide him with proof of payment and the pin number once the transfer was complete. SAMAD told HAQUE to "Tell the brother the senders name is abdul samad and the pin is 29370828." This statement appears to suggest a prior relationship and/or communications between HAQUE and ELSHINAWY. SAMAD then confirmed for HAQUE that he had sent the \$1,500. On March 19, 2015, SAMAD sent an email to HAQUE, to which he attached a receipt from MoneyGram (Post office, Newport, Wales) showing the transfer of \$1,499.99 USD to ELSHINAWY on March 18, 2015, at 17:06 hours.

87. On September 22, 2014, during a Google Hangouts chat session between SAMAD (using samad@ibacs.co.uk) and an individual identified in SAMAD's business accounts as an IBACS developer, the two men discussed the whereabouts of the "Chairman" of their company. UK authorities have indicated that their review of SAMAD's electronic media revealed chats or other exchanges involving SAMAD in which SUJAN was referred to as the "Chairman." In response to the developer's question regarding whether SAMAD could contact SUJAN (the "Chairman"), SAMAD replied that not even HAQUE (referred to as "MD sir") could contact him. The IBACS developer stated, that "all he knew" was that the "Chairman" had said "he was going

to make a turkey office lol We lost him I don't think he will contact us again." The developer ended his statement with a smiling emoticon. SAMAD stated that maybe he had become a "shaheed inshallah," to which the developer raised the question of whether SUJAN went to Syria "with any type of aid for them?" I know from my training and experience that the word "shaheed" is commonly used by terrorists to indicate dying by jihad and "inshallah" is Arabic for God willing. This particular exchange is clearly indicative of SAMAD's and the IBACS developer's knowledge and support of SUJAN affiliation with ISIL's cause.

88. It should be noted that UK investigators were unable to locate any information in the seized documents and electronic evidence from both SAMAD and the IBACS office that reflected creation of an IBACS office in Turkey as discussed in the conversation reference in paragraph 87, and as implied by SAMAD in his police interviews (see paragraph 58). Records of IBACS business meetings in Bangladesh made no reference to any business operations in Turkey; none of the IBACS employee payments showed employees in Turkey being compensated; and the "Credential" files relevant to IBACS businesses had no information regarding an IBACS office in Turkey.

89. Given the above exchanges, there is probable cause to believe that SAMAD has used the samad@ibacs.co.uk account to not only conduct IBACS business, but also to express his support of ISIL's cause, communicate with his criminal associates, and facilitate payments to ELSHINAWY, all of which constitutes evidence, fruits, and instrumentalities of the charged conspiracy.

Google Account: ibacslimited@gmail.com

90. Another email address utilized by SAMAD and associated with IBACS was

ibacslimited@gmail.com. The password for this email address, which was located in the IBACS accounts found in the electronic media seized by UK authorities, was identified as “killobama77.” Also discovered in SAMAD’s seized media was a cartoon drawing depicting President Obama behind a lectern with the caption, “do you know why we do not negotiate with terrorists.” Underneath the cartoon is a picture of President Obama with a distorted face with the caption, “because we are the terrorists.”

91. Investigators in the UK have reviewed some of the content from this account and found (based on their review and their interviews of SAMAD) that certain email addresses for other individuals associated with IBACS appear to have been forwarded to this account. The UK review of the account included emails such as the following:

- An email to shayma.haque@gmail.com in which the sender said that they met at the “madhafa,” which is a term referring to a jihadi boarding house. (Located in the inbox of the ibacslimited@gmail.com account were a number of Facebook notification emails, as recent as November 2015, to shayma.haque@gmail.com. Upon further review, it was discovered that these accounts are linked as these emails are forwarded from shayma.haque@gmail.com to email address ibacslimited@gmail.com.) Shayma HAQUE has been identified as SUJAN’s wife.
- An email dated September 18, 2014, from YouTube to “siful” which included a video from user “Abu Usamah At-Thahabi.” Online research indicated that this person is a UK based speaker who preaches hatred against non-Muslims.
- An email dated August 1, 2015, from Yahoo indicating that an attempt was made to log into Yahoo account “s_lbd” from an unrecognized device in Iraq. Based on my experience, this type of notification would be consistent with ibacslimited@gmail.com having been designated as the recovery email for the Yahoo account “s_lbd.”
- Emails from Facebook dated, respectively, October 3 and November 7, 2015, providing notice that the password on the account had been reset, via email address shayma.haque@gmail.com, from an IP address and device located in Bilgi, Van Province, Turkey.⁴

⁴ Van Province is in the southeastern portion of Turkey. It borders Iran to the east and is north of both

92. This account also contained numerous emails related to the corporate structure of IBACS and its directors. For example, investigators found an email dated July 5, 2014, from Companies House (the organization that registers corporations in the UK) relating to a request for incorporation of “iBacs Corporation Ltd” and its directors.

93. Based on this information, I believe that this email account contains evidence of the mindset of those using this account, access of other accounts from places such as Turkey and Iraq in connection with the charged conspiracy, and information about the corporate structure of IBACS relevant to its use in connection with the charged conspiracy.

Google Account: asamad9134@gmail.com

Twitter Account: [@asamad9134](https://twitter.com/asamad9134)

Facebook account: [asamad91](#)

94. Located on one of SAMAD's seized cell phones were screen captures of several applications utilizing or associated with Google account asamad9134@gmail.com. For example, screen captures of SAMAD's Evernote, Dropbox and Facebook accounts indicated they were 'synced' to this email account. Additionally, a screen capture of the email account's active 'all-inboxes' menu revealed over 99 emails: 10 marked "priority," 18 marked with the label "Islam/Sabeel," 10 marked "important," and 46 marked "sent." Moreover, a screen capture of SAMAD's active Twitter account login to [@asamad9134](https://twitter.com/asamad9134) was also observed. I know from my experience that many times individuals use the same naming convention for multiple accounts. Twitter handle [@asamad9134](https://twitter.com/asamad9134) is identical to the naming convention in asamad9134@gmail.com.

95. During the previously referenced July 3, 2014, Google Hangout chat between SAMAD and SUJAN, SAMAD declared that he was signing up for a Twitter account specifically to obtain radical Islamic content. Investigators in the UK accessed the publically-available portion of SAMAD's Twitter account [@asamad9134](https://twitter.com/asamad9134) and discovered that the account of Anjem Choudary and Moazzam Begg were being "followed" by SAMAD. I know from my experience and training that Anjem Choudary is an ISIL supporter and a Salafi Muslim activist. He was recently convicted in the UK of inciting terrorism (in connection with ISIL) and sentenced to a term of imprisonment of five years. Moazzam Begg was a former Guantanamo Bay detainee who faced charges recently in the UK for traveling to Syria in support of ISIL; the charges have since been dropped.

96. Also discovered within this Twitter account were links to Facebook account [asamad91](#), another account attributed to SAMAD. Investigators in the UK were able to review certain publicly available portions of this Facebook account. On February 10, 2014, a video was

posted to this Facebook account from the Spreading Islam page titled, "HOW ALLAH REWARDS THE SHUHADA (THE MARTYRS) IMAAN BOOSTER!" which was about the rewards for those who die on the battlefield and how every Muslim should aspire to martyrdom. SAMAD commented, "Sit back and relax, and give this 12 minutes of your time." Also observed in the post was a picture of the ISIL flag.

97. On February 15, 2014, SAMAD posted a video to his Facebook account that appears to be a tribute to Anwar Al-Aulaqi. He also posted the comment: "A tribute to my role model of the 21st century: Shiekh Anwar Al-awlaki." As noted above, Al-Aulaqi is a radical Islamic cleric who supported violence against the west.

98. On April 29, 2014, a video was posted to this Facebook account titled "Destruction of Khilafah (Golden age of Islam) Fall of Islamic Empire Documentary." The caption with this video stated "1924 the start of a drastic downfall for the Islamic State. Let's wake up and educate ourselves about history. It is not there for our entertainment but rather a chance to realise and correct what is corrupt." I know from my experience and training that the word, "Khilafah," is Arabic for caliphate. Investigators who reviewed this video described it as aspiring for the return of a caliphate.

99. SAMAD also shared a post over this Facebook account originating from the Spreading Islam Facebook page, which stated, "ALLAHU AKBAR!!! Brother Hamza Andreas Tzortzi's POWERFUL speech outside the Home Office in London ON (02/03/2014) in support of #MoazzamBegg and all the other aseer and oppressed around the world!!"

100. In light of the above-referenced facts, I believe there is probable cause to believe that Twitter account [@asamad9134](#), the Facebook account [asamad91](#), and SAMAD's linked email

account asamad9134@gmail.com contain evidence of SAMAD's involvement in, and mindset with regard to, the charged conspiracy to provide material support to ISIL.

Skype Account: samad.ibacs

101. Located on SAMAD's seized cell phone was a screen capture of SAMAD's Skype account, which was associated with username "[samad.ibacs](#)," the name Abdul SAMAD, and "ibacsGroup.com." Between May and July 2015, SUJAN, SAMAD and HAQUE were involved in the purchase of, and communication about, multiple pieces of FLIR (Forward Looking Infrared)-capable, pan-tilt mounted units from a company in Canada selling military-grade surveillance equipment. The purchase totaled approximately \$18,000 USD. According to the Canadian company's website, the devices are miniature FLIR capable, pan-tilt units that provide accurate real time positioning of cameras, lasers, antennas or other small to medium payloads. Such devices, which are typically used on military and civilian aircraft, use a thermographic camera that senses infrared radiation, thus allowing users to identify target locations, activity and movements. The use of this type of equipment would be inconsistent with IBACS's legitimate business operations.

102. In July 2015, three pan-tilt devices were ordered from the Canadian company and delivered to the IBACS UK office. One of SAMAD's seized phones was found to contain photos – three taken on 7/18/15 and two taken on 9/9/15 – of the pan-tilt units and related equipment laid out on a very distinctive carpet in SAMAD's home that was observed in the same location on the day of his arrest.

103. In a Skype chat on September 14, 2015, between SUJAN and SAMAD (using his Skype account [samad.ibacs](#)), SAMAD confirmed that he had "3 of each items." SUJAN instructed

SAMAD to send “one set” to Madrid, specifically referencing “1 camera, 1 lens, 1 FLIR pantilt system with power supply and control box and the CD.” SUJAN further instructed SAMAD on how to obtain and use a named secure communication platform. SUJAN explained that this platform used a proxy and anonymizer network, along with a different type of operating system, thus rendering communications over the platform totally anonymous and concealed from authorities. SUJAN told SAMAD that they must perform these steps because there was a “security war” between Muslims and “the kuffar.” I know from my experience and training that the word “kuffar” is a derogatory word used to describe non-Muslims. Also located on SAMAD’s seized media was a Skype chat between SAMAD and HAQUE in which HAQUE requested the tracking information for one of the parcels containing the FLIR-related equipment so that he could forward the information to SUJAN.

104. This pan-tilt transaction was ordered through a company called Advance Technology Solutions, also known as Advance Technology Global (hereafter “Advance Tech”). A folder was found within SAMAD’s IBACS business account titled “Daily Report.” It contained reports of activities taken by IBACS web developers, including a task to redesign the Advance Tech website. The tasking, which was dated July 31, 2015, identified the company as a provider of, among other things, robotic drone surveillance and rocket science, oil and gas, water treatment, and food production machinery.

105. During a Skype chat on July 22, 2015, SUJAN told SAMAD (on his samad.ibacs account) that the name of a new holding company he was setting up was AdvanceTech, and he would be using the old IBACS office address as the new company’s address. Advance Technology Global was incorporated in the UK on July 23, 2015. The registered address was the prior Cardiff

address for IBACS and the shareholders were identified as David and Peter Soren. The listed address for Peter Soren is SUJAN's prior UK address. More significantly, the IP address used to log into David SOREN's PayPal account (which lists the IBACS business address in its account registration) was used to log into a PayPal account pertaining to SUJAN.

106. SUJAN and SAMAD discussed the delivery of the pan-tilt equipment during a number of chats in August and September 2015. During one of these chats, there was some discussion about packages having been delivered to the wrong address. SUJAN told SAMAD, "please take care of these my brother, we need those items urgently." He subsequently asked SAMAD to open the packages after they were received in the IBACS office and take photos to send to him so he could confirm the shipment was complete and get a detail on the camera lenses that were included, again noting the urgency of the matter. As he was sending the pictures, SAMAD asked SUJAN, "What's this for ... a sniper?" SUJAN responded, "lol no." SAMAD replied, "Lol Not as exciting as a sniper. Hmmm. Please don't tell me it's to take quality selfies," to which SUJAN responded, "lol no."

107. In a Skype chat on September 16, 2015, SAMAD (using his account samad.ibacs) gave the shipping details of the items to SUJAN and stated, "Is there any way to reduce my services as I can't help but feel a little uneasy?" SUJAN replied, "akhi fillah, I already noticed. May allah guide you. However, as I see what you fear from, I dont ask you anything on that line ... I wish you would only fear Allah alone." SUJAN then quoted an Islamic hadith regarding Allah's protection. In a few subsequent chats, SUJAN asked SAMAD for his contact info on a particular secure messaging platform (known to be used by ISIL) so he could give him some information about why he had been bothering him so much about getting the items shipped. SUJAN also

indicated that some of the items were needed in another country and would be forwarded from Spain once received by an individual to whom SAMAD was directed to send them. (It should be noted that HAQUE left Bangladesh and moved to Spain around August 1, 2015, which he confirmed in another Skype chat with SAMAD.)

108. On July 30, 2015, the David SOREN PayPal account was used to purchase, at a cost of \$381.25 USD, ten rocket flight computer kits to be delivered to Ismail Bayaltun in Sanliurfa, Turkey. This item assists in launching small rockets. The order was arranged through email by an individual identifying himself as Brian Vincer (who also asked the company owner a number of technical questions regarding usage of the device). The contact email address for the order was the AdvanceTech email address discussed above. The shipment was delayed in Turkish customs, prompting Vincer to compose an email stating, "I did a big mistake. The shipping must have been done to the company, not the individual (Ismail Bayaltun) he doesn't work for the company anymore. So now the guys can't get it without him. Can you please see if something could be done from your side." The shipping issue was unable to be resolved and the items were returned and payment refunded in mid-October 2015.

109. The above information provides probable cause to believe that SAMAD's Skype account will contain evidence relating to the conspiracy to provide material support of ISIL. **H.**

Conclusion

110. Based upon the facts set forth in this affidavit, I submit that there is probable cause to believe that within the **Target Accounts**, for the period from January 1, 2014, through December 31, 2015, there exists evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2339B (providing and attempting to provide material support to a foreign terrorist organization)

and 2339C (unlawful financing of terrorism), and conspiracy to commit same.

111. By this affidavit and applications, I request that the Court issue search warrants directed to the service providers allowing agents to seize the e-mail and other information stored on the service providers' servers for the computer accounts and files specified in Attachments A, B, C and D to be searched per the protocol on Attachment E. This court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the court is "a district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

112. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of the requested warrants. The warrants will be faxed to service provider personnel who will be directed to produce those accounts and files.

I. Search Procedure

113. In order to ensure that agents search only those computer accounts and or files described in Section I of Attachments A, B, C and D, this affidavit and the accompanying applications for search warrants seeks authorization to permit employees of the service providers to assist agents in the execution of this warrant. To further ensure that the agents executing the requested warrants search only those computer accounts and/or files described in Section I of Attachments A, B, C and D, the following procedures will be implemented:

a. The search warrant will be presented to the relevant service provider personnel who will be directed to isolate those accounts and files described in Attachments A, B, C and D;

b. In order to minimize any disruption of computer service to innocent third parties, service provider employees (with or without law enforcement personnel) trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Attachments A, B, C and D, including an exact duplicate of all information stored in the computer accounts and files so described;

c. Service provider employees will provide the exact duplicate in electronic form of the accounts and files described in Attachments A, B, C and D, and all information stored in those accounts and files to the agent who serves each warrant;

d. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the service providers' employees and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant, as detailed in Section III of Attachments A, B, C and D; and

e. Law enforcement personnel will then seal the original duplicate of the accounts and files received from service provider employees and will not further review the original duplicate absent an order of the Court.

J. Request for Sealing and Non-Disclosure

114. Since this investigation is continuing, disclosure of the requested search warrants, this affidavit, and the corresponding applications and attachments will jeopardize the progress of the investigation. Accordingly, I request that the Court issue an order that the search warrants, this affidavit, and the corresponding applications and attachments be filed under seal until further order of this Court. In addition, because notification of the existence of this order will seriously jeopardize an investigation, I request that the Court issue an order, pursuant to 18 U.S.C. § 2705(b),

16-3205-ADC

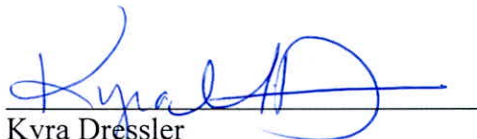
16-3206-ADC

16-3207-ADC

16-3208-ADC

ordering the service providers not to notify any person of the existence of the applications, affidavit, search warrants and attachments, until directed to do so by the Court. Separate motions and orders are being submitted pursuant to these requests. Notwithstanding this nondisclosure order, the government hereby requests permission without further order of this Court to provide copies of the warrant, affidavit and search results to personnel assisting it in the investigation and prosecution of this matter, as well as to appropriate foreign government officials involved in this investigation, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Your affiant has signed this document under oath as to all assertions and allegations contained herein and states that its contents are true and correct to the best of her knowledge.


Kyra Dressler
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 9th day of December, 2016.


United States Magistrate Judge

ATTACHMENT A

I. Facebook Accounts to Be Searched

This warrant seeks to search an account controlled by the free, web-based electronic service provider known as Facebook, Inc. ("Facebook"), headquartered at 1601 California Ave, Palo Alto, California 94304. **The account to be searched bears the following Facebook ID: asamad91 (the "Target Facebook Account").** The information associated with this account is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California.

II. Information to be disclosed by Facebook

To the extent that the information described herein is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the user ID listed in this attachment for the period from January 1, 2014, to December 31, 2015:

(a) All contact and personal identifying information, for the above Facebook IDs : full name, alternate name and name changes, user identification number, birth date, gender, education, languages spoken, physical address (including city, state, and zip code), current city, hometown, work information, contact e-mail addresses (including those removed), credit card information, Facebook passwords, Facebook security questions and answers, telephone numbers, screen names, websites, and other personal identifiers. Group identifiers including group identification number, a list of users currently registered to the group, and Group Contact Info, including all contact

information for the creator and/or administrator of the group and a PDF of the current status of the group profile page.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by those user IDs and all photos and videos uploaded by any user that have those user IDs tagged in them, including any metadata associated with those photos and videos;

(d) All profile and "About Me" information; News Feed information, including Posts by the user or to the user; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists and friend requests, including the friends' Facebook user identification numbers; rejected "Friend" requests; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past events postings; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages sent or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all logins/logouts and records of the IP addresses that logged into the account, and information about active sessions;

(h) The users' last location;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts, all non-Facebook webpages and content that the user has "liked," and all likes on the users' posts, photos, and other content made by others;

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) Chat history;

(l) All past and present lists of friends (including removed or deleted friends), family, and connections;

(m) Any followers or individuals the users are following;

(n) Any information that the users have hidden from their news feeds;

(o) Any shares or status updates;

(p) Linked accounts and screen names;

(q) Notification settings, privacy settings, recent activities;

(r) All records of Facebook searches performed by the account;

(s) All information about the user's access and use of Facebook Marketplace;

(t) The types of service utilized by the user;

(u) Account status history, including the length of service, any activation, deactivation dates, and the means and source of any payments associated with the service (including any credit card or bank account number);

(v) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account; and

(w) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

III. Information to be seized by the government

All information described above in Section II that constitutes fruits, evidence and instrumentalities of violations of 18 USC §§ 2339B and 2339C from January 1, 2014, to December 31, 2015, including, for the user ID identified in this Attachment, information pertaining to the following matters:

(a) Records of communication with other individuals concerning the preparation for, planning of, and/or funding of terrorist-related activities;

(b) Information pertaining to the solicitation and/or identification of co-conspirators and/or facilitators involved or associated with Mohammed ELSHINAWY, Tamer EL-KHODARY, ABDUL SAMAD, ATAUL HAQUE, SIFUL SUJAN, ANA GONZALEZ, SHAYMA AKTER, and others involved in undertaking terrorist-related activity in the United States or elsewhere;

(c) Information pertaining to monetary transfers, financial accounts or other monetary instruments that reasonably appear connected to terrorist-related planning or attacks;

(d) Information about the control and operations of IBACS and its related companies, including Ibacstel Electronics, Advance Technology Solutions (also known as Advance Technology Global ("ATG")), and AdvanceTech;

(e) Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime;

(f) Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(i) The identity of the person(s) who communicated with the user ID about matters relating to supporting terrorist organizations such as ISIL, including records that might help reveal their whereabouts;

(j) Account history (including Terms of Service and any complaints) and billing records (including date, time, duration, and screen names used each time the account was activated).

ATTACHMENT B

I. Twitter Account to Be Searched

This warrant applies to information associated with the Twitter profile with username @asamad9134 that is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered in San Francisco, California.

II. Information to be disclosed by Twitter

To the extent that the information described in this Attachment is within the possession, custody, or control of Twitter, including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in this Attachment for the period from January 1, 2014 through December 31, 2015:

- (a) All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- (b) All past and current usernames, account passwords, and names associated with the account;
- (c) The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- (d) All IP logs and other documents showing the IP address, date, and time of each login to the account;

- (e) All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- (f) All “Tweets” and Direct Messages sent, received, “favorited,” or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;
- (g) All information from the “Connect” tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a list of all Tweets that include the username associated with the account (*i.e.*, “mentions” or “replies”);
- (h) All photographs and images in the user gallery for the account;
- (i) All location data associated with the account, including all information collected by the “Tweet With Location” service;
- (j) All information about the account’s use of Twitter’s link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;
- (k) All data and information that has been deleted by the user;
- (l) A list of all of the people that the user follows on Twitter and all people who are following the user (*i.e.*, the user’s “following” list and “followers” list);
- (m) A list of all users that the account has “unfollowed” or blocked;
- (n) All “lists” created by the account;
- (o) All information on the “Who to Follow” list for the account;
- (p) All privacy and account settings;
- (q) All records of Twitter searches performed by the account, including all past searches saved by the account;

(r) All information about connections between the account and third-party websites and applications;

(s) All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

III. Information to be seized by the government

All information described above in Section II that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2339B and 2339C from January 1, 2014, to December 31, 2015, including, for each user ID identified in this Attachment, information pertaining to the following matters:

(a) Records of communication with other individuals concerning the preparation for, planning of, and/or funding of terrorist-related activities;

(b) Information pertaining to the solicitation and/or identification of co-conspirators and/or facilitators involved or associated with Mohammed ELSHINAWY, Tamer EL-KHODARY, ABDUL SAMAD, ATAUL HAQUE, SIFUL SUJAN, ANA GONZALEZ, SHAYMA AKTER, and others involved in undertaking terrorist-related activity in the United States or elsewhere;

(c) Information pertaining to monetary transfers, financial accounts or other monetary instruments that reasonably appear connected to terrorist-related planning or attacks;

(d) Information about the control and operations of IBACS and its related companies, including Ibacstel Electronics, Advance Technology Solutions (also known as Advance Technology Global ("ATG")), and AdvanceTech;

(e) Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime;

(f) Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(i) The identity of the person(s) who communicated with the user ID about matters relating to supporting terrorist organizations such as ISIL, including records that might help reveal their whereabouts;

(j) Account history (including Terms of Service and any complaints) and billing records (including date, time, duration, and screen names used each time the account was activated).

ATTACHMENT C

I. Gmail Accounts to Be Searched

This warrant applies to information associated with the following electronic accounts:

**info@ibacstel.com
info@ibacs.co.uk
ataul@ibacstel.com
ataul@ibacs.co.uk
ataul03@ibacstel.com
samad@ibacs.co.uk
ibacslimited@gmail.com
asamad9134@gmail.com**

that are stored at premises owned, maintained, controlled, or operated by Google, Inc. ("Google"), headquartered in Mountain View, California.

II. Information to be disclosed by Google, Inc. (the "Provider")

To the extent that the information described in this Attachment is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in this Attachment:

(a) The contents of all emails or other communications (including instant messages, Google Hangouts, and other) associated with the accounts, including stored or preserved copies of emails/communications sent to and from the account, draft emails/communications, the source and destination addresses associated with each email/communication, the date and time at which each email/communication was sent, and the size and length of each email/communication;

(b) The contents of any file storage associated with these accounts, such as Google Drive;

(c) All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

(d) The types of service utilized;

(e) All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

(f) All records pertaining to communications between the Provider and any person regarding the accounts, including contacts with support services and records of actions taken.

III. Information to be seized by the government

All information described above in Section II that constitutes evidence and instrumentalities of violations of 18 U.S.C. §§ 2339B and 2339C from January 1, 2014, to December 31, 2015, including, for each account or identifier listed in this Attachment, information pertaining to the following matters:

(a) Records of communication with other individuals concerning the preparation for, planning of, and/or funding of terrorist-related activities;

(b) Information pertaining to the solicitation and/or identification of co-conspirators and/or facilitators involved or associated with Mohammed ELSHINAWY, Tamer EL-KHODARY, ABDUL SAMAD, ATAUL HAQUE, SIFUL SUJAN, ANA GONZALEZ,

SHAYMA AKTER, and others involved in undertaking terrorist-related activity in the United States or elsewhere;

(c) Information pertaining to monetary transfers, financial accounts or other monetary instruments that reasonably appear connected to terrorist-related planning or attacks;

(d) Information regarding the control and operations of IBACS and its related companies, including Ibacstel Electronics, Advance Technology Solutions (also known as Advance Technology Global (“ATG”), and AdvanceTech;

(e) Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime;

(f) Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner’s state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(i) The identity of the person(s) who communicated with the user ID about matters relating to supporting terrorist organizations such as ISIL, including records that might help reveal their whereabouts;

(j) Account history (including Terms of Service and any complaints) and billing records (including date, time, duration, and screen names used each time the account was activated).

ATTACHMENT D

I. Skype Account to Be Searched

This warrant applies to information associated with the Skype username **samad.ibacs** that is stored at premises owned, maintained, controlled, or operated by Skype, a company headquartered in Luxembourg but owned by Microsoft, Inc., which accepts service of process on behalf of Skype at One Microsoft Way, Redmond, WA 98052-6399.

II. Information to be disclosed by Skype/Microsoft

To the extent that the information described in this Attachment is within the possession, custody, or control of Skype, including any messages, records, files, logs, or information that have been deleted but are still available to Skype, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Skype is required to disclose the following information to the government for each account listed in this Attachment:

- (a) Registration and billing details, including all identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- (b) All past and current usernames, account passwords, and names associated with the account;
- (c) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;
- (d) All IP logs and other documents showing the IP address, date, and time of each login to the account;

- (e) All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- (f) Skype Online Current Subscription: List of Skype Online numbers currently subscribed to by a User;
- (g) Purchase History: Financial transactions conducted with Skype including billing addresses provided;
- (h) All photographs and images in the user gallery for the account;
- (i) All location data associated with the account;
- (j) Skype Out Records: Historical call detail records for calls placed to the public switched telephone network (PSTN);
- (k) All data and information that has been deleted by the user;
- (l) Skype Online Records: Historical call detail records for calls placed from the public switched telephone network (PSTN);
- (m) SMS Records: SMS text message historical detail records;
- (n) Chats and/or instant messages, including the content of any messages and details about the participants and timing of the communications;
- (o) Skype WiFi Records: Historical Skype WiFi records;
- (p) E-mail & Password Records: Historical record of e-mail and password change activity;
- (q) All privacy and account settings;
- (r) All information about connections between the account and third-party websites and applications;

(s) All records pertaining to communications between Skype and any person regarding the user or the user's Skype account, including contacts with support services, and all records of actions taken, including suspensions of the account.

III. Information to be seized by the government

All information described above in Section II that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2339B and 2339C from January 1, 2014, to December 31, 2015, including, for each user ID identified in this Attachment, information pertaining to the following matters:

(a) Records of communication with other individuals concerning the preparation for, planning of, and/or funding of terrorist-related activities;

(b) Information pertaining to the solicitation and/or identification of co-conspirators and/or facilitators involved or associated with Mohammed ELSHINAWY, Tamer EL-KHODARY, ABDUL SAMAD, ATAUL HAQUE, SIFUL SUJAN, ANA GONZALEZ, SHAYMA AKTER, and others involved in undertaking terrorist-related activity in the United States or elsewhere;

(c) Information pertaining to monetary transfers, financial accounts or other monetary instruments that reasonably appear connected to terrorist-related planning or attacks;

(d) Information about the control and operations of IBACS and its related companies, including Ibacstel Electronics, Advance Technology Solutions (also known as Advance Technology Global ("ATG"), and AdvanceTech;

(e) Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime;

(f) Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(i) The identity of the person(s) who communicated with the user ID about matters relating to supporting terrorist organizations such as ISIL, including records that might help reveal their whereabouts;

(j) Account history (including Terms of Service and any complaints) and billing records (including date, time, duration, and screen names used each time the account was activated).

ATTACHMENT E

Description of Methods to be Used for Searching Electronically Stored Information

This warrant authorizes the search of electronically stored information. The search shall be conducted pursuant to the following protocol in order to minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search are viewed.

In order to ensure that agents search only those computer accounts and or files described in Section I of Attachments A, B, C and D, this affidavit and the accompanying applications for search warrants seeks authorization to permit employees of the service providers to assist agents in the execution of this warrant. To further ensure that the agents executing the requested warrants search only those computer accounts and/or files described in Section I of Attachments A, B, C and D, the following procedures will be implemented:

a. The search warrant will be presented to the relevant service provider personnel who will be directed to isolate those accounts and files described in Attachments A, B, C and D;

b. In order to minimize any disruption of computer service to innocent third parties, service provider employees (with or without law enforcement personnel) trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Attachments A, B, C and D, including an exact duplicate of all information stored in the computer accounts and files so described;

c. Service provider employees will provide the exact duplicate in electronic form of the accounts and files described in Attachments A, B, C and D, and all information stored in those accounts and files to the agent who serves each warrant;

d. Law enforcement personnel will thereafter review the information stored in the accounts and files received from the service providers' employees and then identify and copy the information contained in those accounts and files which are authorized to be further copied by this search warrant, as detailed in Section III of Attachments A, B, C and D; and

e. Law enforcement personnel will then seal the original duplicate of the accounts and files received from service provider employees and will not further review the original duplicate absent an order of the Court.